

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-234737

(43)Date of publication of application : 22.08.2003

(51)Int.Cl.

H04L 9/32

(21)Application number : 2002-372602

(71)Applicant : CANON INC

(22)Date of filing : 24.12.2002

(72)Inventor : TONISSON ALAN VALEV

(30)Priority

Priority number : 2001 PR9703

Priority date : 21.12.2001

Priority country : AU

(54) CONTENT AUTHENTICATION FOR DIGITAL MEDIA BASED RECORDING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an enhanced digital file authentication device.

SOLUTION: A method, in a data processing system provided with a recording apparatus and a certificate authority terminal, of determining whether a file is modified, comprises the steps of generating a first public key and a first private key by the recording apparatus, of transferring the first public key to the certificate authority terminal by the recording apparatus, encrypting a certificate including the first public key by using a second private key by the certificate authority terminal, transferring the encoded certificate to the recording apparatus by the certificate authority terminal, hashing the file to provide a digital signature by using the first private key in the recording apparatus, attaching the certificate received from the certificate authority terminal and the digital signature to the file in the recording apparatus, and distributing to a client terminal the file as a communication package assimilated the file, the digital signature and the certificate by the recording apparatus.

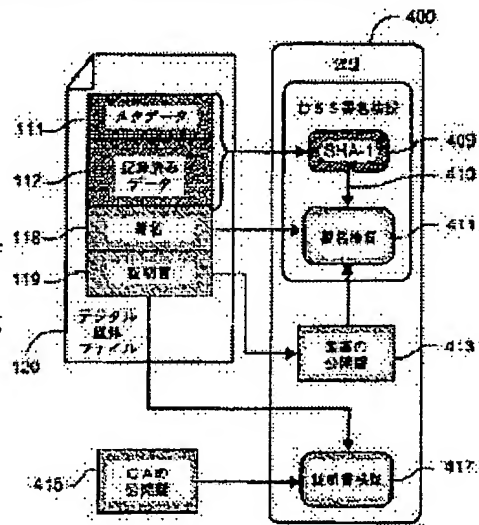


Fig. 4

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-234737
(P2003-234737A)

(43) 公開日 平成15年8月22日 (2003.8.22)

(51) Int.Cl.⁷
H04L 9/32

識別記号

F I
H04L 9/00

テ-マ-ド*(参考)

675D 5J104
675B

審査請求 有 請求項の数10 O L 外国語出願 (全 42 頁)

(21) 出願番号 特願2002-372602(P2002-372602)

(22) 出願日 平成14年12月24日 (2002.12.24)

(31) 優先権主張番号 PR9703

(32) 優先日 平成13年12月21日 (2001.12.21)

(33) 優先権主張国 オーストラリア (AU)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 アラン バレブ トニソン

オーストラリア国 2113 ニュー サウス

ウェールズ州, ノース ライド, ト

ーマス ホルト ドライブ 1 キヤノン

インフォメーション システムズ リサ

ーチ オーストラリア プロプライエタリ

ー リミテッド内

(74) 代理人 100076428

弁理士 大塚 康徳 (外3名)

Fターム(参考) 5J104 AA09 LA03 LA06 MA02

(54) 【発明の名称】 記録装置をはじめとするデジタル媒体のための内容認証

(57) 【要約】 (修正有)

【課題】 改良型のデジタルファイル認証装置を提供する。

【解決手段】 記録装置と認証局端末とを備えるデータ処理システムであり、ファイルが修正されるかを判定する方法であって、前記記録装置によって第一の公開鍵と第一の秘密鍵を生成する行程と、前記記録装置により前記第一の公開鍵を前記認証局端末に転送する行程と、前記認証局端末によって第二の秘密鍵を使用して前記第一の公開鍵を含む証明書を暗号化する行程と、前記暗号化した証明書を前記認証局端末によって前記記録装置に転送する行程と、前記記録装置内の前記第一の秘密鍵を使用して、前記ファイルをハッシングしてデジタル署名を提供する行程と、前記認証局端末から受信した証明書と前記デジタル署名とを前記記録装置内の前記ファイルに添付する行程と、前記記録装置によって前記ファイルとデジタル署名と証明書をを含む通信パッケージとして前記ファイルをクライアント端末に配信する行程を備える。

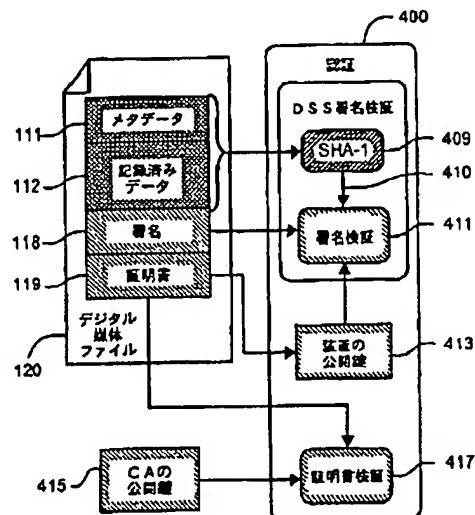


Fig. 4

【特許請求の範囲】

【請求項1】 記録装置と認証局端末とを備えるデータ処理システムにおいて、ファイルが修正されるかどうかを判定する方法であって、

前記記録装置によって第1の公開鍵と第1の秘密鍵とを生成する工程と、

前記記録装置によって前記第1の公開鍵を前記認証局端末に転送する工程と、

前記認証局端末によって第2の秘密鍵を使用して、前記記録装置から受信した前記第1の公開鍵を含む証明書を暗号化する工程と、

前記暗号化した証明書を前記認証局端末によって前記記録装置に転送する工程と、

前記記録装置内の前記第1の秘密鍵を使用して、前記ファイルをハッシングしてデジタル署名を提供する工程と、

前記認証局端末から受信した証明書と前記デジタル署名とを前記記録装置内の前記ファイルに添付する工程と、
前記記録装置によって少なくとも前記ファイルとデジタル署名と証明書をを含む通信パッケージとして前記ファイルをクライアント端末に配信する工程とを備えることを特徴とする方法。

【請求項2】 前記クライアント端末は、

前記認証局端末から受信した第2の公開鍵を使用して前記証明書から前記第1の公開鍵を取得する工程と、

前記第1の公開鍵を使用してデジタル署名を復号化する工程と、

前記ファイルをハッシングしてハッシュを提供する工程と、

前記ハッシュと前記デジタル署名との比較に応じて、前記ファイルが修正されるかどうかを判定する工程とを更に備えることを特徴とする請求項1記載の方法。

【請求項3】 メタデータを生成する工程と、

前記デジタル署名がさらに該メタデータに依存するように該メタデータを前記ファイルと関連付ける工程とを更に備えることを特徴とする請求項1記載の方法。

【請求項4】 前記記録装置のユーザが入力した付加データを受信し、前記付加データを前記メタデータの一部として記憶する工程を更に備えることを特徴とする請求項3記載の方法。

【請求項5】 前記デジタル署名はDSS方法に準拠することを特徴とする請求項1記載の方法。

【請求項6】 記録装置と認証局端末とを備え、ファイルが修正されるかどうかを判定する処理システムであって、

前記記録装置は、

第1の公開鍵と第1の秘密鍵とを生成する生成器と、

前記第1の公開鍵を前記認証局端末に転送する第1の転送器とを備え、

前記認証局端末は、

第2の秘密鍵を使用して、前記記録装置から受信した前記第1の公開鍵を含む証明書を暗号化する暗号器と、
前記暗号化した証明書を前記記録装置に転送する第2の転送器とを備え、

前記記録装置は、

前記第1の秘密鍵を使用して、前記ファイルをハッシングしてデジタル署名を提供する提供器と、

前記認証局から受信した証明書と前記デジタル署名とを前記ファイルに添付する添付手段と、

少なくとも前記ファイルとデジタル署名と証明書を含む通信パッケージとして前記ファイルをクライアント端末に配信する配信器とを備えることを特徴とする処理システム。

【請求項7】 少なくとも秘密鍵と秘密鍵に対応する公開鍵とを備える暗号化鍵対とデジタル証明書を記憶する第1の記憶媒体と、

イベントデータを記録する記録装置と、

少なくとも前記記録されたイベントデータを記憶する第2の記憶媒体と、

少なくとも前記記憶された秘密鍵と前記記録されたイベントデータとを使用して、デジタル署名を生成する署名プロセッサと、

(i) 前記記憶した公開鍵を証明書生成局に供給し、

(ii) 前記公開鍵を使用して形成され、前記証明書生成局から供給された前記デジタル証明書を、少なくとも前記第2の記憶媒体に記憶し、

(iii) イベントデータを記録し、前記署名プロセッサによって生成されたデジタル署名と前記イベントデータとを関連付けるコントローラとを備えることを特徴とする装置。

【請求項8】 認証するデータを処理するデバイスであって、

認証局の秘密鍵から生成したデジタル証明書を受信し、
前記デバイスの公開鍵を組み込む手段と、

前記デバイスの公開鍵を補足してデバイス鍵対をひとまとめに形成する前記デバイスの秘密鍵と、前記データ用のデジタル署名とを生成する手段と、

前記データと前記証明書と前記デジタル署名とを前記デバイスからの転送用の通信パッケージとして関連付ける手段とを備えることを特徴とするデバイス。

【請求項9】 記録装置においてファイルが修正されるかどうかを判定する方法であって、

第1の公開鍵と第1の秘密鍵とを生成する工程と、

前記第1の公開鍵を認証局端末に転送する工程と、

前記第1の秘密鍵を使用して、前記ファイルをハッシングしてデジタル署名を提供する工程と、

前記認証局端末から受信した証明書と前記デジタル署名とを前記ファイルに添付する工程と、

前記記録装置によって少なくとも前記ファイルとデジタル署名と証明書をを含む通信パッケージとして前記ファ

イルをクライアント端末に配信する工程と、を備え、前記認証局端末から受信した証明書は前記第1の公開鍵を含み、前記認証局端末で生成された第2の秘密鍵を使用して暗号化されることを特徴とする方法。

【請求項10】 ファイルが修正されるかどうかを判定するプロセスを実行するためのプログラムを記憶する記憶媒体であって、前記プログラムは、

第1の公開鍵と第1の秘密鍵とを生成する工程と、前記第1の公開鍵を認証局端末に転送する工程と、前記第1の秘密鍵を使用して、前記ファイルをハッシュしてデジタル署名を提供する工程と、前記認証局端末から受信した証明書と前記デジタル署名とを前記ファイルに添付する工程と、前記記録装置によって少なくとも前記ファイルとデジタル署名と証明書とを含む通信パッケージとして前記ファイルをクライアント端末に配信する工程と、を備え、前記認証局端末から受信した証明書は前記第1の公開鍵を含み、前記認証局端末で生成された第2の秘密鍵を使用して暗号化されることを特徴とする記憶媒体。

【発明の詳細な説明】

【0001】【発明の属する技術分野】本発明は、画像及び／又は音声を記録するための記録装置等のデジタル媒体に関し、特に、デジタル記録されたデータとそのデータに関連したメタデータの認証におけるデジタル署名に関する。

【0002】【従来の技術】高品質のデジタル画像や音声を記録するための記録装置等のデジタル媒体が普及している。現在、デジタル媒体に画像や音声を記録する装置には数多くの種類がある。この中には、デジタルステルカメラやデジタルビデオカメラやデジタル音声記録装置が含まれる。これらの装置の相違は、時と共に次第に曖昧になってきている。例えば、最近のデジタルステルカメラの多くは短いモーションシーケンスや音声を記録できるし、デジタルビデオカメラの多くは現在では静止画像を記録できる。

【0003】一般にデジタルカメラでは、電荷結合素子(CCD)センサアレイを撮影場面に露出することでデジタル画像を作成し、通常カメラ内で、CCDが生成したデータをデジタル画像データに変換し、それを記憶媒体に記憶する。デジタルビデオレコーダは、動画を静止画像のシーケンスとして記録するが、記憶する前に圧縮するのが一般的である。音声はマイクを使用して記録し、A/D変換器を使用してデジタルデータに変換する。その後、1つ以上のデジタル媒体ファイルとして装置に記憶されたデジタルデータは、パーソナルコンピュータや、印刷出力用、音声出力用、表示用、送信用などの他の固定記憶装置に転送される。

【0004】しかし、デジタル記録されたデータの1つの問題は、このようなデータは簡単な操作や修正によ

り、本来の場面や出来事に対して偽の表現を作成できてしまうことである。このような問題は、画像や記録音声の正当性を証明することが不可欠な法廷や法施行分野などのある種の分野では、特に深刻になっている。デジタル画像や音声を変更して本来の記録を見かけ上げがめることが簡単であるために、正当性を証明することが困難であることが多く、ときには不可能になってしまうこともある。

【0005】デジタルデータの正当性を証明する従来の手法として、「非対称鍵暗号法」としても知られる公開鍵／秘密鍵暗号法に基づくデジタル署名が使用されている。デジタル署名は、秘密鍵を使用してデジタルデータから生成する。ここでは、通常、秘密鍵によるデータのハッシュを暗号化し、暗号化されたハッシュがデジタル署名を構成する。デジタル署名は、秘密鍵を知らなければ実際に生成することは不可能となるように設計されている。その後は、秘密鍵を知らなくても、対応する公開鍵を使用してデジタル署名を検証することができる。通常、公開鍵を使用して署名を復号化し、その結果として得られたハッシュ値を、署名されたデータから算出されたハッシュと比較することで検証が遂行される。これらのハッシュ値が一致すれば、署名は有効となり、データが署名された際に秘密鍵の所有者が署名されたデータを所有していたことを証明する。

【0006】デジタル署名を検証する場合、使用中の公開鍵が、請求された署名者に実際に属していることを確認する必要がある。鍵の所有者を確認する一手段として、デジタル証明書を使用する。デジタル証明書は、特定の鍵が特定の署名者に属することを表明する認証局

(CA)と呼ばれる信頼できる機関によって発行された電子文書である。証明書には、鍵の所有者を識別する情報や、公開鍵そのものや、認証局のデジタル署名が含まれる。デジタル証明書には、シリアル番号や有効期限などの他の情報が含まれていることが多い。多くの場合、デジタル署名は標準フォーマット(例えば、X.509)に準じており、又、認証中のユーザが署名者の公開鍵を参照できるようにレジストリに保持される。

【0007】記録装置等のデジタル媒体へのデジタル署名の適用例の1つが、米国特許第6,269,446号(Schumacherら)に記載されており、ここではデジタルカメラに適用されている。Schumacherらは、米国特許第5,499,294号(Friedman)に記載された先行技術に改良を加えた。Schumacherらの手法では、デジタルカメラで埋込み秘密鍵を使用し、この秘密鍵を使用して、画像データと関連のメタデータとのメッセージダイジェストに基づくデジタル署名を作成する。この場合、メタデータは、時間と衛星(GPS)位置情報とから導出される。その後、画像データとそれに関連したメタデータの認証を行いたいユーザは、埋込み秘密鍵に対応する公開鍵を取得する。公開鍵を使用することで、Schu

cherらのシステムのユーザは、最初にデジタルカメラで記録されて以来、デジタル画像データが修正されたかどうかを判断することができる。

【0008】Schumacherらのシステムの1つの欠点は、認証中のソフトウェアが、認証が必要とされる画像を有する各カメラの公開鍵を事前に知る必要があるということである。ソフトウェアアプリケーションが多数のカメラからの画像を認証しなければならない場合、このアプリケーションのユーザは、各カメラからの画像を認証する前に、各カメラの公開鍵をソフトウェアに供給しなければならない。このため、多数のカメラや多数の認証ソフトウェアのインスタンスがある場合はSchumacherらのシステムは実用的ではない。多くのアプリケーションにおいて、認証ソフトウェアのユーザが全てのカメラの鍵を取得することは使い勝手が悪い。

【0009】1つの解決策として、全てのカメラが同じ秘密鍵/公開鍵対を備える方法もあるが、システムの機密保護が著しく損なわれてしまう。どれか1つのカメラでもその秘密鍵を漏洩してしまうと、システム全体から秘密鍵が漏洩してしまうため、通常、この解決策を採用することはできない。他の解決策として、鍵と証明書の認証局と公開データベースをそれぞれ1つ以上含むネットワーク化公開鍵インフラストラクチャ(PKI)を使用する。この解決策には、認証中のユーザが公開鍵/証明書データベースにアクセスしなければならないという欠点がある。更に、この解決策では、第三者である認証局が介入する必要があるため、アプリケーションによっては不便なものとなる。

【0010】【発明の概要】本発明の目的は、デジタル媒体ファイルなどのデジタルファイルに対して改良型の認証装置を提供することによって、既存の装置の1つ以上の欠点を実質的に解決する、また少なくとも改善することである。

【0011】この意味で認証とは、媒体ファイル中のデータが、記録装置で記録されて以来、修正されていないことを立証することを意味する。ここでは、「媒体ファイル」という用語を使用して、デジタルスチルカメラ、デジタルビデオカメラ、デジタル録音装置、又は他のデジタル記録装置によって記録されたデータに言及する。媒体ファイルは、記録されたデータに関連したメタデータを含むこともある。かかるメタデータは、原始データとそのキャプチャに関する情報を記述又は提供するデータである。また、メタデータも認証されうる。

【0012】本発明の第1の側面によると、記録装置と認証局端末とを備えるデータ処理システムにおいて、ファイルが修正されるかどうかを判定する方法であって、前記記録装置によって第1の公開鍵と第1の秘密鍵とを生成する工程と、前記記録装置によって前記第1の公開鍵を前記認証局端末に転送する工程と、前記認証局端末によって第2の秘密鍵を使用して、前記記録装置から受

信した前記第1の公開鍵を含む証明書を暗号化する工程と、前記暗号化した証明書を前記認証局端末によって前記記録装置に転送する工程と、前記記録装置内の前記第1の秘密鍵を使用して、前記ファイルをハッシングしてデジタル署名を提供する工程と、前記認証局端末から受信した証明書と前記デジタル署名とを前記記録装置内の前記ファイルに添付する工程と、前記記録装置によって少なくとも前記ファイルとデジタル署名と証明書を含む通信パッケージとして前記ファイルをクライアント端末に配信する工程とを備えることを特徴とする方法を提供する。

【0013】本発明の他の側面によると、記録装置と認証局端末とを備え、ファイルが修正されるかどうかを判定する処理システムであって、前記記録装置は、第1の公開鍵と第1の秘密鍵とを生成する生成器と、前記第1の公開鍵を前記認証局端末に転送する第1の転送器とを備え、前記認証局端末は、第2の秘密鍵を使用して、前記記録装置から受信した前記第1の公開鍵を含む証明書を暗号化する暗号器と、前記暗号化した証明書を前記記録装置に転送する第2の転送器とを備え、前記記録装置は、前記第1の秘密鍵を使用して、前記ファイルをハッシングしてデジタル署名を提供する提供器と、前記認証局から受信した証明書と前記デジタル署名とを前記ファイルに添付する添付手段と、少なくとも前記ファイルとデジタル署名と証明書を通信パッケージとして前記ファイルをクライアント端末に配信する配信器とを備えることを特徴とする処理システムを提供する。

【0014】本発明の他の側面によると、少なくとも秘密鍵と秘密鍵に対応する公開鍵とを備える暗号化鍵対とデジタル証明書とを記憶する第1の記憶媒体と、イベントデータを記録する記録装置と、少なくとも前記記録されたイベントデータを記憶する第2の記憶媒体と、少なくとも前記記憶された秘密鍵と前記記録されたイベントデータとを使用して、デジタル署名を生成する署名プロセッサと、(i)前記記憶した公開鍵を証明書生成局に供給し、(ii)前記公開鍵を使用して形成され、前記証明書生成局から供給された前記デジタル証明書を、少なくとも前記第2の記憶媒体に記憶し、(iii)イベントデータを記録し、前記署名プロセッサによって生成されたデジタル署名と前記イベントデータとを関連付けるコントローラとを備えることを特徴とする装置を提供する。

【0015】本発明の他の側面によると、認証するデータを処理するデバイスであって、認証局の秘密鍵から生成したデジタル証明書を受信し、前記デバイスの公開鍵を組み込む手段と、前記デバイスの公開鍵を補足してデバイス鍵対をひとまとめに形成する前記デバイスの秘密鍵と、前記データ用のデジタル署名とを生成する手段と、前記データと前記証明書と前記デジタル署名とを前記デバイスからの転送用の通信パッケージとして関連付

ける手段とを備えることを特徴とするデバイスを提供する。

【0016】本発明の他の側面によると、記録装置においてファイルが修正されるかどうかを判定する方法であって、第1の公開鍵と第1の秘密鍵とを生成する工程と、前記第1の公開鍵を認証局端末に転送する工程と、前記第1の秘密鍵を使用して、前記ファイルをハッシングしてデジタル署名を提供する工程と、前記認証局端末から受信した証明書と前記デジタル署名とを前記ファイルに添付する工程と、前記記録装置によって少なくとも前記ファイルとデジタル署名と証明書をを含む通信パッケージとして前記ファイルをクライアント端末に配信する工程と、を備え、前記認証局端末から受信した証明書は前記第1の公開鍵を含み、前記認証局端末で生成された第2の秘密鍵を使用して暗号化されることを特徴とする方法を提供する。

【0017】本発明の他の側面によると、ファイルが修正されるかどうかを判定するプロセスを実行するためのプログラムを記憶する記憶媒体であって、前記プログラムは、第1の公開鍵と第1の秘密鍵とを生成する工程と、前記第1の公開鍵を認証局端末に転送する工程と、前記第1の秘密鍵を使用して、前記ファイルをハッシングしてデジタル署名を提供する工程と、前記認証局端末から受信した証明書と前記デジタル署名とを前記ファイルに添付する工程と、前記記録装置によって少なくとも前記ファイルとデジタル署名と証明書をを含む通信パッケージとして前記ファイルをクライアント端末に配信する工程と、を備え、前記認証局端末から受信した証明書は前記第1の公開鍵を含み、前記認証局端末で生成された第2の秘密鍵を使用して暗号化されることを特徴とする記憶媒体を提供する。

【0018】本発明の他の側面も開示されている。

【0019】有利な実施形態では、デジタル記録装置は、あとで送信するために内部媒体に記憶された、又は外部デジタル記憶媒体に直接送信された媒体ファイルを生成する手段だけでなく、まず、媒体ファイル中の全て又は一部のデータのデジタル署名を生成して、デジタル証明書を記憶する手段をも備えている。装置が生成したデジタル署名は、デジタル記録装置に記憶された秘密鍵に依存する。秘密鍵は、デジタル記録装置のメーカー以外は誰も知らない。媒体ファイル中のデータを認証するために、ユーザは、記録装置の秘密鍵に対応する公開鍵を知らなければならない。ソフトウェアが公開鍵を取得して、公開鍵自体が正規のものであることを確認できるためには、公開鍵と、公開鍵の正当性を証明するデジタル証明書とを、デジタル記録装置が生成した媒体ファイルに付加する。証明書は、供給された公開鍵がデジタル記録装置に記憶された秘密鍵に対応する有効な公開鍵であることを証明する他のデジタル署名を含む。

【0020】【最良の態様を含む詳細な説明】図1A

は、記録要の画像、音声、又はその両方を取り込むためのセンサ150を含むデジタル記録装置100を示す。装置100は、更に、処理装置（又はCPU）160を介して装置100の動作を制御するプログラム命令を記憶するための読み出し専用メモリ（ROM）109などの不揮発性記録媒体を含む。CPU160は、ROM109から得られた命令を読み込んで実行する。CPU160は、取り込んだ画像や音声情報をセンサ150から抽出し、例えば、磁気ディスクドライブ、光磁気ドライブ、又はフラッシュROMなどにより構成される不揮発性デジタル大容量記憶媒体108に同一形式で保存するように動作する。ROM109の機能を記憶媒体108に内蔵する実施形態もある。ランダムアクセスメモリ

（RAM）180も図示されており、鍵や署名や証明書を処理するための（揮発性の）中間記憶容量をCPU160に提供する。有線ケーブル、光ケーブル、又は無線周波数や赤外線リンクなどの無線方法で形成される外部接続195に対して、取り込まれた画像や音声データを、記録装置100から通信モジュール190を介して出力してもよい。部品160～190を1つの集積回路チップ装置に形成する実施形態もある。

【0021】図1Bは、記録装置100の主要な機能部品と、接続195を介して出力するデジタル媒体ファイル120を生成するためにどのようにこれらの部品を使用するのかわかる。デジタル記録装置100は、記録要の画像や音声をそれぞれ検出するための画像センサ101とマイク102を内蔵しており、図示された構成では、画像センサ101とマイク102が図1Aのセンサ150を形成している。通常、装置100はセンサ101に光を集光するためにレンズ（不図示）も含み、センサ101は一時的に画像データバッファ103に記憶するデジタル輝度データを生成するように動作する。通常、輝度データは、赤と緑と青の成分からなる。その後、JPEG、JPEG2000、又はMPEGなどの適切な圧縮機能105を使用して輝度データを圧縮するのが好ましく、その結果得られた圧縮データ112を、デジタル記憶媒体108中のデジタル媒体ファイル120の一部として記憶する。図示のように、音声情報をマイク102によって同時に検出し、音声データバッファ104に一時的に記憶する前にA/D変換器（ADC）121によってデジタル音声データに変換することができる。音声データも、MP3などの適切な圧縮機能105を使用して圧縮し、記録済みのデータ112にデジタル媒体ファイル120の一部として付加する。バッファ103と104をRAM180や専用のメモリを使用して実現してもよいし、圧縮機能をCPU160や特定のハードウェア装置（不図示）で適切に行ってもよい。他の実施形態として、画像バッファ103又は音声バッファ104は存在せず、音声や画像データを圧縮して直接、デジタル記憶媒体108に書き込んでもよい。更な

る実施形態では、記録済みのデータ112を非圧縮音声及び/又は画像データで形成するように圧縮機能105を省略してもよい。マイク102と、ADC121と、音声データバッファ104とが存在しない実施形態もあるし、画像センサ101と画像データバッファ103とが存在しない実施形態もある。

【0022】図1Bに示すように、記録装置100は、記録済みのデータ112に関連したメタデータ111を生成するように構成されたモジュール106を含む。メタデータ111は、データが記録された日時や、記録が行われたGPS位置座標の他、露出設定やテキストデータ入力などのユーザが特定したデータを含んでもよい。メタデータ111はデジタル媒体ファイル120の一部として記憶される。この機能を省略し、デジタル媒体ファイル120にメタデータを記憶しない実施形態もある。

【0023】秘密鍵113と公開鍵114とデジタル証明書115とは、フラッシュROMなどの不揮発性書き換え可能記憶装置に記憶するのが好ましく、この記憶装置は記憶媒体108やその一部を形成するように使用してもよい。代わりに、そのデータをROM109に記憶してもよく、その場合、データが改竄されたり変更されたりすることはないが、認証局において変更ができず、ユーザがローカル認証局を維持できないという欠点がある。また、メーカーには鍵の管理に対する責任が生じ、ユーザは鍵の生成するメーカーを信用しなければならない、これらの理由から、要求に応じて記録装置100に新しい鍵を生成させるのが好ましいが、これは鍵113と114及び証明書115の書き換えを必要とする。秘密鍵113は、高性能で安全性の高いアプリケーションにおける改竄防止ハードウェアにオプションとして記憶してもよい。公開鍵114は、通常、証明書115に含まれているので、図1Bの114に示されるように、公開鍵のコピーを別に記憶する必要は厳密にはない。しかし、証明書115とは別に公開鍵114を記憶することで、デジタル証明書115を使用しない可能性も見込める。このように、証明書115の使用は任意であり、記録装置100が証明書115の形式を知らなくてもよくなる。

【0024】また、図1Bに示すように、署名生成サブプロセス117で秘密鍵113を使用してデジタル署名118を生成し、デジタル媒体ファイル120の一部として記憶するプロセス107を実行するようにCPU160が動作する。デジタル署名プロセス107は、米国国立標準技術研究所(NIST)によって特定された既知のデジタル署名標準(DSS)に準拠するのが好ましい。プロセス107では、CPU160が、署名するデータのSHA-1ハッシュ機能116を計算し、それによってハッシュ結果130を提供する。SHA-1ハッシュ機能116の後に署名生成プロセス117を実行

し、具体的にはハッシュ結果130を秘密鍵113で暗号化する。図示の構成では、署名されたデータには、データ131としてまとめて図示された記録済みのデータ112と関連のメタデータ111とが含まれている。他の実施形態では、署名されたデータ131が記録済みのデータ112を全て含んでいなくてもよいし、関連のメタデータ111を全て含んでいなくてもよい。

【0025】また、図1Bに示すように、生成した署名118をデジタル媒体ファイル120に付加するのと同様に、CPU160は証明書挿入機能110に従って、証明書115のコピー119をデジタル媒体ファイル120に付加する。

【0026】通常の物理的な実施形態では、圧縮機能105とSHA-1ハッシュ機能116をアプリケーション特有の集積回路で行うのが好ましく、残りの機能は便宜的にCPU160で実現してもよい。

【0027】デジタル媒体ファイル120が記録装置100によってひとたび形成されると、メタデータ111と記録済みのデータ112と署名118と証明書119とを備えたデジタル媒体ファイル120は、CPU160によって装置100から出力される。これによって、図5に示すように、ファイル120を記憶装置108から通信モジュール190とリンク195とを介してコンピュータシステム500に転送することができる。図示のように、リンク195は、(破線のラインを介して)直通でもよいし、コンピュータネットワーク520を介していてもよい。

【0028】記録済みのデータ112とメタデータ111の認証は、汎用のコンピュータシステム500上で動作するソフトウェアアプリケーションによって行うのが好ましい。ここでは、認証プロセスを、コンピュータシステム500内で実行するアプリケーションプログラムなどのソフトウェアとして実現する。実際、プロセスのステップは、コンピュータが実行するソフトウェアの命令によって達成される。命令は、各々が1つ以上の特定のタスクを行うための1つ以上のコードモジュールからなる。ソフトウェアを2つ別々の部分に分割してもよく、その場合、第1の部分の部分が認証方法を行い、第2の部分部分が第1の部分とユーザとの間のユーザインタフェースを管理する。ソフトウェアを、後述の記憶装置などを含むコンピュータ可読媒体に記憶してもよい。ソフトウェアは、コンピュータからコンピュータ可読媒体に読み込まれた後、コンピュータによって実行される。このようなソフトウェアやコンピュータプログラムが記録されたコンピュータ可読媒体は、コンピュータプログラム製品である。コンピュータでコンピュータプログラム製品を使用することによって、記録済みのデータを認証するための有利な装置を達成するのが好ましい。

【0029】コンピュータシステム500は、コンピュータモジュール501と、キーボード502やマウス5

03などの入力装置と、プリンタ515を含む出力装置と、表示装置514と、スピーカー517とを具備する。変調復調モデムトランシーバ装置516は、コンピュータモジュール501が、例えば、電話線521や他の機能媒体を介して接続可能なコンピュータネットワーク520と通信するために使用する。モデム516を使用してインターネットや、ローカルエリアネットワーク（LAN）や広域ネットワーク（WAN）などの他のネットワークシステムにアクセスすることができる。適切な場合には、ネットワークカード（不図示）で、コンピュータモジュール501とLANやWANとの間を直接接続するI/Oインタフェース508の一部を形成してもよい。

【0030】図示のように、コンピュータモジュール501は、通常、少なくとも1つのプロセッサ505と、例えば、半導体ランダムアクセスメモリ（RAM）や読み出し専用メモリ（ROM）からなるメモリ装置506と、表示装置514やスピーカー517のためのオーディオ・ビデオ・インタフェース507とキーボード502やマウス503やオプションとしてのジョイスティック（不図示）のためのI/Oインタフェース513とを含む入出力（I/O）インタフェースと、モデム516や直接デバイス接続のためのインタフェース508とを含む。記憶装置509が提供されており、通常、ハードディスクドライブ510とフロッピーディスクドライブ511とを含む。磁気テープドライブ（不図示）を使用してもよい。CD-ROMドライブ512は、通常、不揮発性のデータソースとして提供される。コンピュータモジュール501の部品505～513は、関連技術で既知のコンピュータシステム500の動作の従来のモードが得られるように、通常、相互接続されたバス504を介して通信する。前述の構成を実施できるコンピュータの例としては、IBMのPCやその互換機、Sun Sparcstationsやそこから発展した同等のコンピュータシステムを含む。

【0031】通常、アプリケーションプログラムは、ハードディスクドライブ510に常駐し、実行する際にプロセッサ505によって読み出されて制御される。プログラムや、ネットワーク520から取り込まれたデータの一時的な記憶は、半導体メモリ506を使用して、可能ならばハードディスクドライブ510と協力して遂行してもよい。場合によっては、アプリケーションプログラムをCD-ROMやフロッピーディスク上で符号化してユーザが供給し、対応するドライブ512や511から読み出してもよいし、又は、ユーザがネットワーク520からモデム装置516を介して読み出してもよい。更に、ソフトウェアを、他のコンピュータ可読媒体からコンピュータシステム500に読み込むこともできる。ここで使用する「コンピュータ可読媒体」という用語は、実行及び/又は処理を行うために、命令及び/又は

データをコンピュータシステム500に提供することに関わる記憶装置や伝送媒体を含む。記憶媒体の例としては、記憶媒体がコンピュータモジュール501の内部にあるのか外部にあるのかに関わらず、フロッピーディスク、磁気テープ、CD-ROM、ハードディスクドライブ、ROM又は集積回路、光磁気ディスク、PCMCIAカードなどのコンピュータ可読カードが挙げられる。伝送媒体の例としては、他のコンピュータやネットワーク化装置へのネットワーク接続と同様に無線伝送路や赤外線伝送路と、Eメール送信とウェブ上などに記録された情報を含むインターネットやイントラネットとが挙げられる。

【0032】代わりに、認証方法を、認証の機能やサブ機能を行う1つ以上の集積回路などの専用ハードウェアで実現してもよい。このような専用ハードウェアは、図形プロセッサ、デジタル信号プロセッサ、又は1つ以上のマイクロプロセッサと関連のメモリを含んでもよい。

【0033】デジタル媒体ファイル120をコンピュータモジュール501にダウンロードし、例えばHDD510に記憶することで、データ111と112を記録した装置100の公開鍵114を事前に知らなくても、証明書119によって認証アプリケーションが、データ111と112を含むデジタル媒体ファイルを認証することができる。

【0034】これを達成する最も簡単な方法は、ある認証者によって画像を認証する全ての記録装置に対して証明書を生成するのに同じ認証局を使用することである。その後、認証局の公開鍵のみを使用して認証を行うことができる。単一の認証局を使用することが実用的でない場合であっても、証明書を使用することで、認証者（すなわち、コンピュータ500や、認証アプリケーションや、そのユーザ）が信用しなければならない公開鍵の数を削減することができる。好適な実施形態では、1つ以上の認証局の公開鍵を、認証に使用するソフトウェアに記憶する。例えば、認証局560によって操作され、且つ、ネットワーク520に接続されたサーバコンピュータ550から、コンピュータシステム500のユーザが、ソフトウェアをダウンロードすることで、このようなソフトウェアを認証局から取得することができる。

【0035】図2は、公開鍵と秘密鍵と証明書の作成に関わるステップを示す。図2に示すように、記録装置100は、公開鍵114と秘密鍵113とからなる暗号化/復号化鍵対を生成する機能201を更に有する。鍵113と114は、2048ビット以上の長さを有するRSA秘密鍵/公開鍵対を構成するのが好ましい。代わりに、他の暗号化アルゴリズムの鍵を使用してもよい。例えば、RSAの代わりに、楕円曲線暗号化アルゴリズムを使用してもよい。他の実施形態では、鍵113と114は装置100のメーカーが生成し、製造過程で証明書115と共に装置100に埋め込んでもよい。しかし、

鍵113と114は、記録装置100が生成し、不揮発性記憶装置109に記憶するのが好ましい。

【0036】図2に示すように、ユーザが公開鍵114のコピー207を認証局560に証明用に送ることができるように、記録装置100は、記憶された公開鍵114にアクセスする手段をユーザに提供する。認証局560は、例えば、サーバコンピュータ550で機能211を操作し、記録装置100の証明書インポート機能219を使用してユーザに供給した後、前述の証明書115として記憶することができるデジタル証明書217を生成する。証明書217は、認証局560の秘密鍵215を使用して作成する。また、証明書217はX.509標準に準拠するのが好ましい。有利な点として記録装置100は、インポートの際に証明書217を解析したりチェックしたりしないため、記録装置100を修正しなくとも想定していなかった形式を含む1つ以上の証明書の形式をサポートする。記録装置100のユーザは、通常、公開鍵114又は207に関連した情報213も認証局560に供給する。この点に関して、証明書217は、証明書217が作成された時間などの、鍵114又は207のオーナーに関する種々の情報を含んでもよい。鍵114又は207のオーナーは、証明書217が証明する情報は正しいものであり、特に、公開鍵114又は207はユーザが所有する秘密鍵113に対応していることを認証局560に証明しなければならない。前述の実施例の場合、このことは、装置100のオーナーが、装置100を認証局560に示し、装置100が与える公開鍵114又は207を示すことによって達成してもよい。鍵114又は207に関連した「オーナー」という用語は、「装置」そのものか、装置を有する「人物」のどちらかを意味するものであってもよい。これは、証明書217が何を証明しようとしているかに依存する。アプリケーションの中には、どちらを使ってもよいものがある。情報213は、少なくとも記録装置100の固有シリアル番号（又はデバイスID）を含み、公開鍵207は供給されたシリアル番号を使って装置100が生成したという証明を認証局560に与えるのが好ましい。このため、前述のように、記録装置100のシリアル番号を証明書217に含めることができる。他の実施形態では、他の情報を供給して公開鍵207のオーナーを識別してもよい。鍵207と情報213を転送するために、記録装置100は、コンピュータシステム500を利用して、あるいは例えばI/Oインタフェース508への直接接続195を使用する媒介のような異なるコンピュータネットワークを利用してよい。代わりに、通信モジュール190の高度化レベルに応じて、装置100とサーバ550との間の通信を、ネットワーク520を介して直接、確立してもよい。代わりに、鍵を手動でサーバ550に入力してもよい。

【0037】装置100が、証明書115として証明書

217のコピーをひとたび記憶すると、記録装置100は認証可能なデータを記録する準備が整う。

【0038】図3は、鍵と証明書の生成とインストールとに関わる方法300をフローチャートとしてまとめたものである。方法300は、通常、可能であればコンピュータシステム500と協力して記録装置100やCAサーバ550上で動作する多数のソフトウェアプログラムとして実現してもよく、これらは種々のユーザアクションに応じて動作し、開始ステップ301より処理が開始される。その後のステップ303において、ユーザは、鍵対を生成するように装置100に信号を送る。これは、図1Aに示すように、装置100に配置された適切なユーザインタフェース185を使用することで行われる。ステップ305において、記録装置100は鍵対113と114を生成するが、これは、図2に示す機能201を使用して遂行される。ステップ307において、生成した公開鍵114をユーザ配布用に供給するように、ユーザはユーザインタフェース185を操作して記録装置100に再度、信号を送る。これに応じて、ステップ309において、装置100は、公開鍵114のコピー207をユーザに受け渡す。これは、パーソナルコンピュータ500を介して供給してもよいし、例えば、装置100のRAM180のユーザアクセス可能位置に供給してもよい。ステップ311において、ユーザは公開鍵のコピー207を付加情報213と共にコンピュータ500又はRAM180から認証局560に、例えばサーバ550経由で供給する。ステップ313において、認証局560は、図2の機能215を使用して証明書217を生成し、ステップ315において、証明書217をユーザに供給する。また、コンピュータ500を介して供給してもよいし、装置100のRAM180に直接供給してもよい。ステップ317において、ユーザは、インタフェース185を介して装置100に証明書217を証明書115として記憶するように指示を出す。これは、図2の証明書インポート機能219を介して行われる。ステップ319において、装置100は証明書115を記憶し、ステップ321でこの方法を終了する。

【0039】図4は、好適な実施形態によるデジタル媒体ファイル120の認証に関わるデータとステップを示す。これらのステップは、パーソナルコンピュータシステム500上で動作するソフトウェアアプリケーション400によって行われるのが好ましく、例えば、前述のように、コンピュータシステム500に適用された、デジタル媒体ファイル120の検証に関わる独立した2つの主要なプロセスを含む。第1のプロセスでは、デジタル署名118が有効な署名であることを検証する。第2のプロセスでは、ファイル120に含まれる証明書119が本物であることを検証する。好適な実施形態では、署名検証プロセスはデジタル署名標準（DSS）に準拠

する。他の実施形態では、他のデジタル署名方式を使用してもよい。

【0040】デジタル署名118を検証する第1のプロセスでは、まず、ファイル120に記憶されたメタデータ111と記録済みのデータ112とのハッシュを算出する。このハッシュは、DSSが特定するSHA-1アルゴリズム409を使用して算出する。ハッシュ結果410を、記録装置100の公開鍵114の抽出バージョン413と共に、DSS署名検証プロセス411への入力として使用する。抽出公開鍵413は、デジタル媒体ファイル120に記憶された証明書119から取得し、これから、公開鍵114(207)が証明書217、115、又は119の一部として保存されていたことが再現される。署名の検証は、再生された公開鍵413を使用して署名118を復号化し、復号化した署名をハッシュ結果410と比較するように動作する機能411によって行われる。両者が同じであれば、ファイル120は正規なものとなる。最後の検証ステップも、DSS署名検証方法に応じて行うのが好ましい。

【0041】証明書119を検証する第2のプロセスでは、認証局560の公開鍵415を使用して証明書119のデジタル署名を検証する機能417を使用する。ここでは、装置の公開鍵413は必要ない。証明書の公開鍵が、ファイルを認証するのに使用する公開鍵と一致することをチェックしたいだけだからである。しかし、前述の構成では、公開鍵(413)を証明書119から取得しているため、鍵413に別にアクセスする必要はない。証明書119は、認証局560の公開鍵415を使用して検証され、装置100の公開鍵114(413)は証明書119のデータの一部にすぎない。証明書119はX.509認証形式に準じるのが好ましいが、X.509証明書での使用に適したデジタル署名方式を使用してもよい。

【0042】[産業への適用性] このことから、認証の検証が望まれるデータの取り込みと記録に前述の構成を適用できることは明らかである。これは、コンピュータ産業やデータ処理産業に普及しており、特に、コンピュータネットワークに接続される可能性のあるカメラなどの携帯型データ取り込み装置に関連している。

【0043】本発明のいくつかの実施形態を説明してきたが、本発明の範囲から逸脱することなく修正と変更のうち少なくともいずれかが可能であり、前述の実施形態は例示的なものであり限定的なものではない。

【0044】本発明者と本出願人は、従来例の開示に関連した[従来技術]の記載が、単に公知の知識としての開示に関するものであり、この記載が、この開示がオーストリアなどで周知の一般的な知識の全て又は一部を示しているということを本発明者や本出願人が承認しているとして構成されるものではないということを特筆しておく。

【図面の簡単な説明】

【図1A】本実施形態に係る記録装置の構造を表す概略ブロック図である。

【図1B】図1Aの記録装置を表す機能ブロック図である。

【図2】図1A及び1Bの記録装置の公開鍵と秘密鍵と証明書の作成とインストールに関するデータとステップを示す図である。

【図3】鍵と証明書の生成とインストールに関するステップをより詳細に示す図である。

【図4】図1A及び1Bのデジタル記録装置によって生成されたデジタル媒体ファイルを認証するプロセスを示す図である。

【図5】図1A及び1Bの記録装置と通信するために前述の鍵と証明書を生成することができるコンピュータシステムの概略ブロック図である。

【図3】

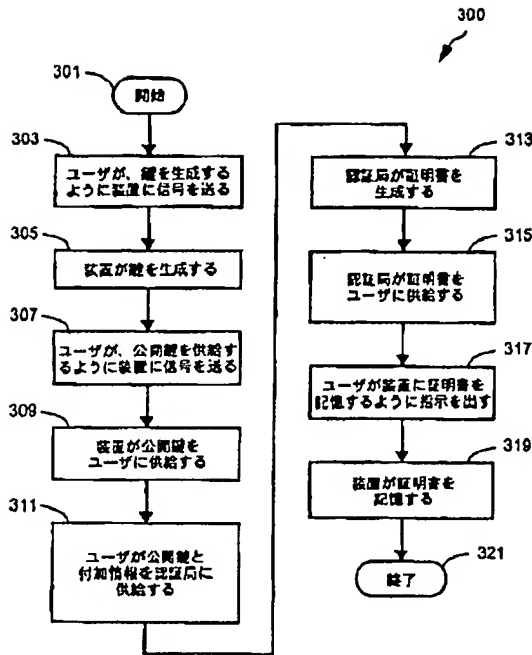


Fig. 3

【図5】

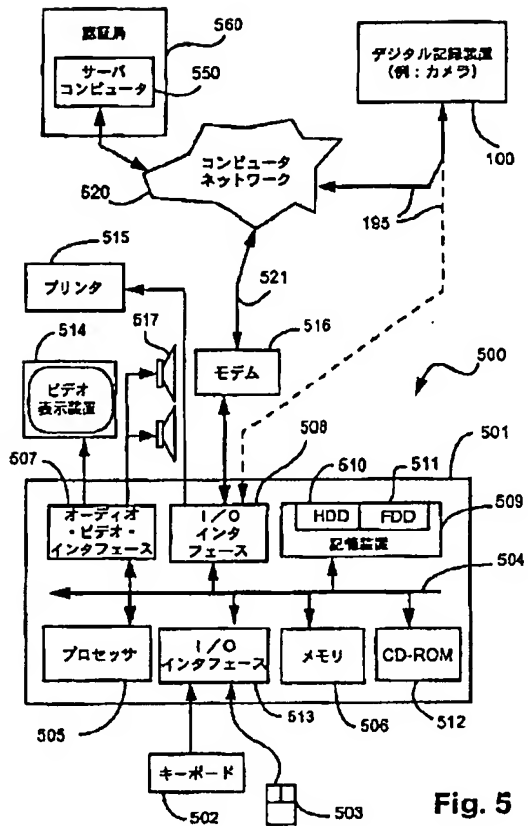


Fig. 5